WHAT IS CLAIMED IS:

Sub A1

~~1. A system for detecting and selectively removing viruses in data transfers, the system comprising:~~

~~a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus;~~

~~a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output; and~~

~~a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted.~~

2. The system of claim 1, wherein the server includes:

27

~~a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input, a data output and a control output, the data input coupled to receive the data to be transferred; and~~

~~a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output, the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred.~~

Sub A2

~~3. The system of claim 2, wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node.~~

~~4. The system of claim 2, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node.~~

~~5. A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:~~

~~receiving at a server a data transfer request including a destination address;~~

~~electronically transmitting data to the server;~~

~~determining whether the data contains a virus at the server;~~

~~performing a preset action on the data using the server if the data contains a virus; and~~

~~sending the data to the destination address if the data does not contain a virus.~~

3 ~~6~~. The method of claim 4 ~~5~~, further comprising the steps of storing the data in a temporary file at the server after the step of electronically transmitting; and wherein the step of determining includes scanning the data for a virus using the server.

Sub A3

~~7. The method of claim 6, wherein the step of scanning is performed using in signature scanning process.~~

7 ~~8~~. The method of claim 4 ~~5~~, wherein the step of performing a preset action on the data using the server comprises performing one step from the group of:

transmitting the data unchanged;

not transmitting the data; and

storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

~~9. The method of claim 5, further comprising the steps of:~~

~~determining whether the data is of a type that is likely to contain a virus; and~~

~~transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus.~~

Sub A4

~~10. The method of claim 9 wherein the step of determining whether the data is of a type that is likely to contain a virus is performed by comparing an extension type of a file name for the data to a group of known extension types.~~

9 ~~11~~. The method of claim 4 ~~5~~, further comprising the steps of:

determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;

wherein the server is a FTP proxy server;

β wherein the step of electronically receiving ~~transmitting~~ data comprises the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network; and

β wherein the step of electronically receiving ~~transmitting~~ data comprises the steps of transferring the data from a server task to an FTP daemon, and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network.

10 ~~12~~. The method of claim 4 ~~5~~, further comprising the steps of:

determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;

wherein the server is a FTP proxy server;

wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network; and

wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network.

Sub A5

~~13. A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:~~

~~receiving a mail message request including a destination address;~~

~~electronically transmitting the mail message to a server;~~

~~determining whether the mail message contains a virus;~~

~~performing a preset action on the mail message if the mail message contains a virus; and~~

~~sending the mail message to the destination address if the mail message does not contains a virus.~~

~~14. The method of claim 13, wherein the step of determining whether the mail message contains a virus is performed by scanning the mail message for encoded portions.~~

Sub A6

~~15. The method of claim 14, wherein the step of scanning the mail message for encoded portions searches for uuencoded portions.~~

~~16. The method of claim 14, wherein:~~

~~the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions;~~

~~the server includes a SMTP proxy server and a SMTP daemon; and~~

~~the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon, and transferring the mail message from the SMTP daemon to a node having an address matching the destination address.~~

14 ~~17~~. The method of claim 11 ~~12~~ ~~13~~, wherein the step of determining whether the mail message contains a virus, further comprises the steps of:

storing the message in a temporary file;

scanning the temporary file for viruses; and

testing whether the scanning step found a virus.

~~18. The method of claim 13, wherein the step of determining whether the mail message contains a virus, further comprises the step of:~~

~~determining whether the mail message contains any encoded portions;~~

~~storing each encoded portion of the mail message in a separate temporary file;~~

~~decoding the encoded portions of the mail message to produced decoded portions of the mail message;~~

~~scanning each of the decoded portions for a virus; and~~

~~testing whether the scanning step found any viruses.~~

Sub A7

~~19. The method of claim 18, wherein step of scanning is performed using in signature scanning process.~~

31

20. The method of claim 14, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

transferring the mail message unchanged;

not transferring the mail message; and

storing the mail message as file with a new name and notifying a recipient of the mail message request of the new file name; and

creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.

21. The method of claim 18, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

transferring the mail message unchanged;

transferring the mail message with the encoded portions having a virus deleted; and

renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory; and

writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message.

18 ~~22~~. An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:

means for receiving a data transfer request including a destination address;

B means for electronically receiving ~~transmitting~~ data at ~~to~~ a server;

means for determining whether the data contains a virus at the server;

means for performing a preset action on the data using the server if the data contains a virus; and

means for sending the data to the destination address if the data does not contain a virus.

Sub A8 ~~23. The apparatus of claim 22, wherein means for determining includes a means for scanning that scans the data using in a signature scanning process.~~

20 ~~24~~. The apparatus of claim 18 ~~22~~, wherein the means for performing a preset action comprises:

means for transmitting the data unchanged;

means for not transmitting the data; and

means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

21 ~~25~~. The apparatus of claim 18 ~~22~~, further comprising:

a second means for determining whether the data is of a type that is likely to contain a virus; and

means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus.

22 ~~26~~. The apparatus of claim 18 ~~22~~, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network.